UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/075,471	02/13/2002	Jeffrey M. Ayars	REAL-2006051 (RN65)	7533

61857 7590 06/25/2008
AXIOS LAW GROUP, PLLC / REALNETWORKS, INC
1525 FOURTH AVENUE
SUITE 800
SEATTLE, WA 98101

EXAMINER	
PALIWAL, YOGESH	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
06/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/075,471	AYARS ET AL.	
	Examiner	**Art Unit**	
	YOGESH PALIWAL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 March 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) *34-42* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

- Applicant's amendment filed on March 17, 2008 has been entered. Applicant has amended claims 1, 18, 25, and 29. Currently claims 1-42 are pending in this application. Claims 34-42 are withdrawn.

Docketing

1. Please note that the application has been re-docketed to different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the office action.

Response to Arguments

2. Applicant's arguments with respect to claims 1, 18, 25 and 29 have been considered but are moot in view of the new ground(s) of rejection.

Also note that previous office action indicated that claims 12-17 are allowed and claims 2-4, 7, 11, 24, 26-28 and 30 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form. However, updated search of prior art has revealed a pertinent prior art and these claims have now been rejected with new ground(s) of rejection.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 25-26 are rejected under 35 U.S.C. 102(e) as being anticipated by England et al. (US 6,775,779 B1), hereinafter England.

Regarding **Claim 25**, England discloses a processor implemented method comprising:

verifying with a root one of a plurality of hierarchically organized digital content rendering modules (see, Fig. 4, Numeral 441), that each module that occupies an immediate downstream position in the hierarchy of modules from the root module has not been compromised (see Column 8, lines 25-35) , during an initialization period (Column 11, line 12);

exclusively receiving with the root one of the plurality of hierarchically organized digital content rendering modules a first digital content of a first type (See Column 11, lines 6-31);

rendering in part with said root one of said modules said first digital content (See Column 11, lines 6-31); re-verifying with said root one of said modules that one of the at least one other one of the modules occupying an immediate downstream position in the hierarchy of modules from the root module is uncompromised (see Column 8, lines 25-35, Column 11, line 12); and

transferring with said root one of said modules the first digital content to the re- verified immediate downstream module to further the rendering of the first digital content (see Column 8, lines 25-35).

Regarding **Claim 26**, the rejection of claim 25 is incorporated and England further discloses wherein said root one verifies each immediate downstream module is uncompromised by verifying the immediate downstream module's signature (see England, Column 8, lines 42-46).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over England.

Regarding **Claim 27**, the rejection of claim 25 is incorporated and England does not explicitly disclose wherein:

the root one of the plurality of hierarchically organized plain text digital content rendering modules receiving a second protected digital content of the same first type; and

said root one in conjunction with the same first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with said root ones re-verifying the same one of the first at least one other one that occupies an immediate downstream position in the hierarchy of modules from the root module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

Above limitations are identical to claim 25 with the difference that this time it is done on a second protected digital content of the same first type.

Since the system of England is capable to receiving different types of digital contents (see England Column 7, lines 57-60), it would have been obvious at the time invention was made to one of ordinary skill in the art to perform the identical steps for the second protected digital content of the same first type as well, to provide secure loading of second protected digital content with the help of security manager of England's device.

Regarding **Claim 28**, the rejection of claim 25 is incorporated and the combination of England and Graunke does not explicitly discloses:

the root one of the plurality of hierarchically organized plain text digital content rendering modules receiving a second protected digital content of a second type; and

said root one in conjunction with second at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with said root one re-verifying one of the second at least one other one occupying an immediate downstream position in the hierarchy of modules from the root module is uncompromised before transferring the second digital content to the re-verified one of the second at least one other one occupying an immediate downstream position in the hierarchy of modules from the root module to further the rendering of the second digital content.

Above limitations are identical to claim 25 with the difference that this time it is done on a second protected digital content of a second type.

Since the system of England is capable to receiving different types of digital content (see England Column 7, lines 57-60), it would have been obvious at the time invention was made to one of ordinary skill in the art to perform the identical steps for the second protected digital content of the second type as well, to provide secure loading of second protected digital content with the help of security manager of England's device.

Claims 1-24, and 29-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over England in view of Graunke et al. (US 5,991,399), hereinafter Graunke.

Regarding **Claim 1**, England discloses an apparatus comprising:

a tamper resistant digital content recovery module (Fig. 4, Numeral 420, Column 9, lines 52-54) to recover protected digital content of various type (see Column 14, lines 18-34), the recovery module employing measure to hinder observation of operations performed therein (see, Column 3, lines 31-42);

a plurality of plain text digital content rendering modules communicatively coupled with each other in a hierarchical manner forming a hierarchy of modules (see, Fig. 4, Numeral 441, 460, 451, also see Column 8, lines 35-52), with selective combinations of the plain text digital content rendering modules to be selectively employed to render the recovered digital contents of the various types (see, Column 8, lines 25-34), including one of the plain text digital content rendering modules occupying a root position of the hierarchy to exclusively receive all types of the recovered digital contents to be rendered (see, Column 12, lines 25-39),

one or more storage units operative to store said tamper resistant module (see, Column 13, lines 60-62) and said plurality of plain text digital content rendering modules (see, Fig. 4, Numerals 441, 460, and 451); and

a processor coupled with the one or more storage units to execute the tamper resistant module and the plurality of plain text digital content rendering modules (see, Fig. 1, Numeral 131).

Tamper resistant digital content recovery module of England simply verifies the root module and provide root module with the decryption key. Therefore, root module of England does not recover the content from the tamper resistant digital content recovery module but only receive the decryption keys and then it decrypts the content itself. Therefore, England does not explicitly discloses one of the plain text digital content rendering modules occupying a root position of the hierarchy to exclusively receive all types of the recovered digital contents to be rendered, <u>from the tamper resistant digital content recovery module</u>.

However, it is common in the art of cryptography to use tamper resistant digital content recovery module to not only verify and supply decryption keys but actually performing the decryption by the temper resistant module and returning the decrypted content to content rendering modules.

Graunke discloses a temper resistant module (see Fig. 2, Numeral 52) that performs the decryption of the encrypted digital content and return the decrypted content (upon verification of the rendering module) to the rendering module (see Fig. 4B, Numerals 124 and 130).

Therefore, it would have been obvious at the time invention was made to one of ordinary skill in the art to perform, with security manager of England, not only the verification and generation of decryption keys but also perform the actual decryption of the content by the security manager, as taught by Graunke because it improves the security of the apparatus of England by not transmitting the decryption keys to even trusted module so that trusted modules wont be able to re-render the encrypted document at a later time without the help of security manager.

Regarding **Claim 2**, the rejection of claim 1 is incorporated and the combination of England and Graunke further discloses wherein the tamper resistant digital content recovery module is equipped to verify the plain text digital content rendering module occupying the root position of the hierarchy as not having been compromised, and to provide recovered digital content to the plain text digital content rendering module occupying the root position of the hierarchy, only upon having verified the plain text digital content rendering module occupying the root position of the hierarchy as not having been compromised (see England, Column 8, lines 9-18).

Regarding **Claim 3**, the rejection of claim 2 is incorporated and the combination of England and Graunke further discloses wherein the tamper resistant digital content recovery module is equipped to verify the plain text digital content rendering module occupying the root position of the hierarchy, responsive to a request from the plain text digital content rendering module occupying the root position of the hierarchy to recover a protected digital content (see England, Column 11, lines 6-31).

Regarding **Claim 4**, the rejection of claim 3 is incorporated the combination of England and Graunke further discloses the tamper resistant digital content recovery module is equipped to verify the plain text digital content rendering module occupying the root position of the hierarchy by verifying a signature of the plain text digital content rendering module occupying the root position (see England, Column 8, lines 42-46).

Regarding **Claim 5**, the rejection of claim 1 is incorporated and the combination of England and Graunke further discloses the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf plain text digital content rendering module, and the non-leaf module is equipped to verify the immediate downstream module as not having been compromised (see England, Fig. 4 and also Column 8 lines 25-35).

Regarding **Claim 6**, the rejection of claim 5 is incorporated and the combination of England and Graunke further discloses wherein the non-leaf modules is equipped to verify the immediate downstream module as not having been compromised, at least during initialization (see England, Column 11, lines 11-13).

Regarding **Claim 7**, the rejection of claim 6 is incorporated and the combination of England and Graunke further discloses wherein the non-leaf modules is equipped to further verify the immediate downstream module remains un-compromised before each transfer of recovered digital content to the immediate downstream module (see England, Column 11, lines 20-31).

Regarding **Claim 8**, the rejection of claim 5 is incorporated and the combination of England and Graunke further discloses wherein the a non-leaf modules is equipped to verify the immediate downstream module as not having been compromised by verifying a signature of the immediate downstream module (see England, Column 8, lines 42-46).

Regarding **Claim 9**, the rejection of claim 1 is incorporated and the combination of England and Graunke further discloses wherein the digital content of various types comprises streaming media contents of a plurality of media, and of a plurality of format types (see England, Column 7, lines 56-60).

Regarding **Claim 10**, the rejection of claim 1 is incorporated and the combination of England and Graunke further discloses wherein the apparatus is a selected one of a wireless mobile phone, a palm sized personal digital assistant, a notebook computer, a set-top box, a desktop computer, a single processor server, a multi-processor server, or a cluster of coupled systems (see England, Fig. 1).

Regarding **Claim 11**, the rejection of claim 1 is incorporated and the combination of England and Graunke further discloses a first subset of the plain text digital content rendering modules are member modules of a first application domain (see England, Fig. 4, Numeral 441), and a second subset of the plain text digital content rendering modules are member modules of a second application domain (see England, Fig. 4, Numerals 460 and 451).

Regarding **Claim 12**, England discloses a processor implemented method, comprising:

a root one of a plurality of hierarchically organized plain text digital content rendering modules (see, Fig. 4, Numeral 441) collectively adapted to render digital contents of a plurality of types (see Column 12, lines 25-27);

verifying with the tamper resistant digital content recovery module that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been compromised (see, Column 8, lines 9-18);

rendering with said root one in conjunction with first at least one other one of said plurality of hierarchically organized plain text digital content rendering modules said first digital content (see, Column 10, lines 28-33); and

verifying with said root one of the modules that one of the first at least one other one of the modules occupying an immediate downstream position in the hierarchy of modules from the root module, is uncompromised before transferring the first digital content to the verified immediate downstream module to further the rendering of the first digital content (see, Column 8, lines 25-35).

Tamper resistant digital content recovery module of England simply verifies the root module and provide root module with the decryption key. Therefore, root module of England does not recover the content from the tamper resistant digital content recovery module but only receive the decryption keys and then it decrypts the content itself. Therefore, England does not explicitly requesting a tamper resistant digital content recovery module to recover a first protected digital content of a first type; recovering with the tamper resistant digital content recovery module the first protected digital content in an obfuscated manner; and transferring the recovered first digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules.

However, it is common in the art of cryptography to use tamper resistant digital content recovery module to not only verify and supply decryption keys but actually performing the decryption by the temper resistant module and returning the decrypted content to content rendering modules.

Graunke discloses a temper resistant module (see Fig. 2, Numeral 52) that performs the decryption of the encrypted digital content and return the decrypted content (upon verification of the rendering module) to the rendering module (see Fig. 4B, Numerals 124 and 130).

Therefore, it would have been obvious at the time invention was made to one of ordinary skill in the art to perform, with security manager of England, not only the verification and generation of decryption keys but also perform the actual decryption of the content by the security manager, as taught by Graunke because it improves the security of the apparatus of England by not transmitting the decryption keys to even trusted module so that trusted modules wont be able to re-render the encrypted document at a later time without the help of security manager.

Regarding **Claim 13**, the rejection of claim 12 is incorporated and the combination of England and Graunke further discloses wherein the tamper resistant module verifies the root one of the plurality of hierarchically organized plain text digital content rendering modules by verifying the root one's signature (see England, Column 8, lines 42-46).

Regarding **Claim 14**, the rejection of claim 12 is incorporated and the combination of England and Graunke further discloses wherein said root one verifies the one of the first one other one that occupies an immediate downstream position in the hierarchy of modules from the root module is uncompromised by verifying the immediate downstream module' s signature (see Column 8, lines 25-35 and lines 42-46).

Regarding **Claim 15**, the rejection of claim 13 is incorporated and the combination of England and Graunke further discloses wherein the method further comprises said root one verifies each module occupying an immediate downstream position in the hierarchy of modules from the root modules (see England, Column 8, lines 25-35) during initialization (see Column 11, line 12).

Regarding **Claim 16**, the rejection of claim 16 is incorporated and the combination of England and Graunke does not disclose wherein:

the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module to recover a second protected digital content of the same first type;

the tamper resistant digital content recovery module verifying that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been compromised;

the tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and

said root one in conjunction with the same first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with said root one re-verifying the same immediate downstream module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

Above limitations are identical to claim 12 with the difference that this time it is done on a second protected digital content of the same first type.

Since the system of England is capable to receiving different types of digital content (see England Column 7, lines 57-60), it would have been obvious at the time invention was made to one of ordinary skill in the art to perform the identical steps for the second protected digital content of the same first type as well, to provide secure loading of second protected digital content with the help of security manager of England's device.

Regarding **Claim 17**, the rejection of claim 12 is incorporated and the combination of England and Graunke does not explicitly discloses:

the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module to recover a second protected digital content of a second type;

the tamper resistant digital content recovery module verifying that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been compromised;

the tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and

said root one in conjunction with second at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with said root one verifying one of the second at least one other one occupying an immediate downstream position in the hierarchy of modules from the root module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

Above limitations are identical to claim 12 with the difference that this time it is done on a second protected digital content of a second type.

Since the system of England is capable to receiving different types of digital content (see England Column 7, lines 57-60), it would have been obvious at the time invention was made to one of ordinary skill in the art to perform the identical steps for the second protected digital content of the second type as well, to provide secure loading of second protected digital content with the help of security manager of England's device.

Regarding **Claim 18**, England discloses an apparatus comprising:

a plurality of digital content rendering modules communicatively coupled with each other in a hierarchical manner forming a hierarchy of modules (see, Fig. 4, Numerals 441, 460, 451), with selective combinations of the modules to be selectively employed to protectively render digital content of various types (see, Column 11, lines 17-31), including one of said digital content rendering modules occupying a root position of the hierarchy (see, Fig. 4, Numeral 441) to exclusively receive the various types of digital contents to be rendered, using a recovery module (see Fig. 4, Numeral 420) not part of the hierarchy of modules, the recovery module employing measures to hinder observation of operations performed therein (Column 11, lines 52-54), and the root modules being operative for verifying a module occupying an immediate downstream position in the hierarchy of modules from the root module as not having been compromised (see, Column 8, lines 25-35);

one or more storage units to store said plurality of digital content rendering modules (Fig. 1, numerals 110, 150, 151, 152); and a processor coupled with the one or more storage units to execute the digital content rendering modules (see, Fig. 1, numeral 131).

Tamper resistant digital content recovery module of England simply verifies the root module and provide root module with the decryption key. Therefore, root module of England does not recover the content from the tamper resistant digital content recovery module but only receive the decryption keys and then it decrypts the content itself. Therefore, England does not explicitly discloses a root position of the hierarchy to exclusively receive the various types of digital contents to be rendered, from a recovery module the recovery module being responsible for recovering the digital contents from their ciphered states.

However, it is common in the art of cryptography to use tamper resistant digital content recovery module to not only verify and supply decryption keys but actually performing the decryption by the temper resistant module and returning the decrypted content to content rendering modules.

Graunke discloses a temper resistant module (see Fig. 2, Numeral 52) that performs the decryption of the encrypted digital content and return the decrypted content (upon verification of the rendering module) to the rendering module (see Fig. 4B, Numerals 124 and 130).

Therefore, it would have been obvious at the time invention was made to one of ordinary skill in the art to perform, with security manager of England, not only the verification and generation of decryption keys but also perform the actual decryption of the content by the security manager, as taught by Graunke because it improves the security of the apparatus of England by not transmitting the decryption keys to even trusted module so that trusted modules wont be able to re-render the encrypted document at a later time without the help of security manager.

Regarding **Claim 19**, the rejection of claim 18 is incorporated and the combination of England and Graunke further discloses wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf module, and the non-leaf module is equipped to verify the immediate downstream module as not having been compromised (see England, Column 8, lines 25-35), at least during initialization (see Column 11, line 12).

Regarding **Claim 20**, the rejection of claim 18 is incorporated and the combination of England and Graunke further discloses wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf module, and the non-leaf modules is equipped to further verify to the immediate downstream module remains uncompromised before each transfer of digital contents to the immediate downstream digital content rendering module (see England, Column 8 lines 25-35 and Column 8, lines 42-46).

Regarding **Claim 21**, the rejection of claim 21 is incorporated and the combination of England and Graunke further discloses wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf module, and the non-leaf module is equipped to verify the immediate downstream module as not having been compromised, by verifying a signature of the immediate downstream modules (see England, Column 8, lines 42-46).

Regarding **Claim 22**, the rejection of claim 18 is incorporated and the combination of England and Graunke further discloses wherein the digital content of various types comprises streaming media contents of a plurality of media, and of a plurality of format types (see England, Column 7, lines 56-60).

Regarding **Claim 23**, the rejection of claim 18 is incorporated and the combination of England and Graunke further discloses wherein the apparatus is a selected one of a wireless mobile phone, a palm sized personal digital assistant, a notebook computer, a set-top box, a desktop computer, a single processor server, a multi-processor server, or a cluster of coupled systems (see England, Fig. 1).

Regarding **Claim 24**, the rejection of claim 18 is incorporated and the combination of England and Graunke further discloses a first subset of the plain text digital content rendering modules are member modules of a first application domain (see England, Fig. 4, Numeral 441), and a second subset of the plain text digital content rendering modules are member modules of a second application domain (see England, Fig. 4, Numerals 460 and 451).

Regarding **Claim 29**, England discloses an article of manufacture comprising:

a recordable medium (see Fig. 1, Numerals 110, 151, 152);

a first plurality of programming instructions recorded on said recordable medium, said first programming instructions adapted to program a computing device to implement on the computing device a tamper resistant digital content recovery module (Fig. 4, Numeral 420, Column 9, lines 52-54) to recover protected digital contents of various types (see Column 14, lines 18-34), the recovery module employing measures to hinder observation of operations performed therein (see, Column 3, lines 31-42); and

a second plurality of programming instructions recorded on said recordable medium (see, Fig. 4, Numeral 441, 460, 451, also see Column 8, lines 35-52), said second programming instructions operative to program a computing device to implement on the computing device a plurality of plain text digital content rendering modules (see, Column 8, lines 25-34), said rendering modules communicatively coupled with each other in a hierarchical manner to form a hierarchy of modules the plain text digital content rendering modules being selectively employed in combination to render the recovered digital contents of the various types (see, Column 8, lines 25-35) including one of the plain text digital content rendering modules occupying a root position of the hierarchy (see, Fig. 4, Numeral 441) to exclusively receive all types of the recovered digital contents to be rendered (See Column 11, lines 6-31).

a root position of the hierarchy (see, Fig. 4, Numeral 441) to exclusively receive all types of the recovered digital contents to be rendered from the tamper resistant digital content recovery module

Tamper resistant digital content recovery module of England simply verifies the root module and provide root module with the decryption key. Therefore, root module of England does not recover the content from the tamper resistant digital content recovery module but only receive the decryption keys and then it decrypts the content itself. Therefore, England does not explicitly disclose a root position of the hierarchy to exclusively receive all types of the recovered digital contents to be rendered from the tamper resistant digital content recovery module.

However, it is common in the art of cryptography to use tamper resistant digital content recovery module to not only verify and supply decryption keys but actually performing the decryption by the temper resistant module and returning the decrypted content to content rendering modules.

Graunke discloses a temper resistant module (see Fig. 2, Numeral 52) that performs the decryption of the encrypted digital content and return the decrypted content (upon verification of the rendering module) to the rendering module (see Fig. 4B, Numerals 124 and 130).

Therefore, it would have been obvious at the time invention was made to one of ordinary skill in the art to perform, with security manager of England, not only the verification and generation of decryption keys but also perform the actual decryption of the content by the security manager, as taught by Graunke because it improves the security of the apparatus of England by not transmitting the decryption keys to even trusted module so that trusted modules wont be able to re-render the encrypted document at a later time without the help of security manager.

Regarding **Claim 30**, the rejection of claim 29 is incorporated and the combination of England and Graunke further discloses wherein the tamper resistant digital content recovery module is equipped to verify the plain text digital content rendering module occupying the root position of the hierarchy as not having been compromised, and to provide recovered digital content to the plain text digital content rendering module occupying the root position of the hierarchy, only upon having verified the plain text digital content rendering module occupying the root position of the hierarchy as not having been compromised (see England, Column 8, lines 9-18).

Regarding **Claim 31**, the rejection of claim 29 is incorporated and the combination of England and Graunke further discloses wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf plain text digital content rendering module, and the non-leaf module is equipped to verify the immediate downstream module as not having been compromised (see England, Fig. 4 and also Column 8 lines 25-35).

Regarding **Claim 32**, the rejection of claim 30 is incorporated and the combination of England and Graunke further discloses the digital content of various types, comprises streaming media contents of a plurality of media, and of a plurality of format types (see England, Column 7, lines 56-60).

Regarding **Claim 33**, the rejection of claim 33 is incorporated and the combination of England and Graunke further discloses the recordable medium is a selected one of a magnetically recordable medium and an optically recordable medium (see, Fig. 1, Numerals 110, 151 and 152).

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2135
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135